IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CHANELLE ZIMMERMAN, BARBARA STEETLE, ROBERT WARUSZEWSKI, WENDY MARSHALL, ANGELA HOLLANDSWORTH, and KEVIN HARRISON individually, and on behalf of all others similarly situated, Plaintiffs, v. HIGHMARK, INC., a Pennsylvania Corporation, Defendant.	Case No. 2:23-cv-250-NR

OPINION

J. Nicholas Ranjan, United States District Judge

These days, a single, inadvertent click on an email can spawn a multitude of class-action lawsuits. That's what happened here.

In December 2022, a Highmark employee was sent an email with a link. That employee clicked on the link. Unbeknownst to that person, the email had been sent by a malicious actor, "phishing" for prey. The link opened a virtual door for the bad actor to obtain access to a treasure trove of Highmark customers' sensitive information. Names, addresses, email addresses, phone numbers, passport numbers, social security numbers, medical treatment information, and financial information—all compromised. Much of it very valuable. Some of it could be sold for profit on the so-called "dark web."

Data breaches, especially in the health-care industry, are becoming very common. So too the class-action litigation that follows. After the Highmark data breach, Plaintiffs here filed suit against Highmark. In the operative first amended complaint, Plaintiffs allege that Highmark failed to safeguard Plaintiffs' and class

members' personally identifiable information ("PII") and protected health information ("PHI"), leading to a data breach that violated Plaintiffs' and class members' privacy rights.

Plaintiffs seek damages for negligence (Count I), negligence *per se* (Count II), breach of fiduciary duty (Count III), breach of confidence (Count IV), breach of implied contract (Count V), and unjust enrichment (Count VI), and also seek a declaratory judgment that Highmark owed a duty to secure the class members' data and that Highmark breached that duty (Count VII). Plaintiffs also seek injunctive relief mandating that Highmark employ adequate security protocols.

Highmark now moves the Court to dismiss the case. Highmark claims that Plaintiffs do not have standing and that Plaintiffs have failed to state any viable claims. After careful consideration, the Court finds that Plaintiffs do, in fact, have standing to bring their claims. The main sticking point for standing in data-breach cases is the injury-in-fact requirement. Plaintiffs here have sufficiently pled an injury in fact, by pleading an intentional breach, misuse of the data, and the sensitive nature of the data at issue. As to the merits of the claims, Plaintiffs properly state claims for Counts I, V, VI, and VII; but Highmark is right that Plaintiffs' claims for Counts II, III, and IV fail, at least as pled, as a matter of law. So the Court will grant the motion in part and deny it in part.

BACKGROUND

On February 6, 2023, Highmark announced that it had experienced a data breach. ECF 32, ¶ 49. According to Highmark, this data breach was the result of a malicious phishing attack in December 2022, which compromised an employee's email account and allowed an unauthorized third party to access confidential information. *Id.* at ¶¶ 50-51. The impacted information included: "members' Social Security Numbers, and enrollment information such as the individual's group name, identification number, and claims or treatment information such as claim numbers,

dates of service, procedures, and prescription information, as well as in some cases, financial information, addresses, phone numbers, and email addresses." *Id.*, ¶ 52.

Plaintiffs allege that Highmark discovered the data breach on December 15, 2022, but did not disclose the data breach to the public until February 6, 2023. *Id.*, ¶ 7. Plaintiffs allege that because of the data breach, they are at a significantly increased risk of fraud, identity theft, misappropriation of health-insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief. *Id.*, ¶ 10. Plaintiffs allege that Highmark "failed to implement reasonable data security measures" to protect their PII and PHI from hackers. *Id.*, ¶ 27. According to the complaint, the healthcare industry is especially susceptible to phishing attacks, which is the type of attack that led to the data breach. *Id.*, ¶¶ 58-61. Plaintiffs allege that they have expended time and money to take steps to try and protect their data after the breach, including spending time looking at credit card accounts, freezing accounts, dealing with actual fraudulent activity, and purchasing protective services, such as LifeLock. *Id.*, ¶¶ 103, 106, 109, 111, 113, 116.

Against this backdrop, Plaintiffs sued Highmark. Plaintiffs are seeking damages and declaratory and injunctive relief for their claims, which include negligence, negligence *per se*, breach of fiduciary duty, breach of confidence, breach of implied contract, unjust enrichment, and declaratory judgment. *Id.*, Prayer for Relief, ¶¶ (a)-(h).

As noted above, after the filing of the consolidated amended complaint, Highmark moved to dismiss. ECF 35. The Court received full briefing on the motion (ECF 36; ECF 38; ECF 39), so it is now ready for disposition.

STANDARD OF REVIEW

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (cleaned up). "A claim has facial

plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* Any reasonable inferences should be considered in the light most favorable to the plaintiff. *See Lula v. Network Appliance*, 255 F. App'x 610, 611 (3d Cir. 2007) (citing *Rocks v. City of Phila.*, 868 F.2d 644, 645 (3d Cir. 1989)).

DISCUSSION & ANALYSIS

I. Plaintiffs have Article III standing.

Highmark initially contends that Plaintiffs lack standing to bring any of their claims. To establish standing under Article III, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). "The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements." *Id.*

The Court addresses each of these three requirements, in turn.

A. Injury in fact

The first requirement for standing is that the plaintiff suffered an injury in fact—that is, an injury that is at least: (i) either actual or imminent, and (ii) concrete.[1] *Id.* at 339. For many years, courts have grappled with the contours of an injury in fact in data-breach cases. The reason the issue has been tricky is that in virtually all of these cases, the actual injury to a plaintiff, if any, will not have materialized or matured until well into the future. For example, a stolen credit card today may not cause any harm to the cardholder until a few months later when it is sold on the dark web to other bad actors. So, the questions are: how likely is it for the risk of harm to

[1] The injury must also be particularized, but that is not at issue here, as the injuries pled are obviously particularized to Plaintiffs; that is, they are not merely generalized grievances. *See, e.g.*, *Spokeo*, 578 U.S. at 339 ("For an injury to be particularized, it must affect the plaintiff in a personal and individual way." (cleaned up)).

materialize? And, is it so likely (or imminent) that Article III standing exists to bring a claim now?

About three years ago, the Third Circuit developed a helpful rubric for courts to assess these issues in data-breach cases. *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152 (3d Cir. 2022). As has always been the case, for an injury in fact to exist, the injury must be at least imminent and concrete. *Id.* at 152, 154. For imminence (which is usually the harder issue), the Third Circuit identified some useful (albeit non-exhaustive) guideposts: (1) "whether the data breach was intentional[;]" (2) "whether the data was misused[;]" and (3) "whether the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft." *Id.* at 153-54. Applying these guideposts here, the Court has no trouble in concluding that Plaintiffs have pled an imminent harm.

Intentional breach. The amended complaint pleads that the data breach here was the product of an intentional attack—*i.e.*, a malicious email phishing campaign by an unauthorized third party. ECF 32, ¶ 50 ("According to Highmark, on or around December 13, 2022, a malicious phishing link led to the compromise of an employee's email."); ¶ 58 ("Phishing is a type of cyberattack used to trick individuals into divulging sensitive information via electronic communication, such as email, by impersonating a trustworthy source.").

Misuse. The amended complaint alleges that at least some of Plaintiffs' data has already been misused. For example:

- "Plaintiff Zimmerman received a notification that her personal information was found on the Dark Web around February 17, 2023." ECF 32, ¶ 102.
- "Plaintiff Waruszewski experienced actual attempted fraud in that someone used his Discover card to make a purchase from Facebook on

March 17, 2023, and later attempted to purchase something from GrubHub on March 21, 2023." *Id.*, ¶ 108.

- "Plaintiff Hollandsworth experienced actual and attempted fraud on various accounts which she was notified of through LifeLock, including: (i) notification that an application online for Red Stone Credit was made in her name, (ii) a hard hit on her credit report which she had to dispute, (iii) an attempt made for a loan from Wells Fargo (of which she is not a current customer), (iv) someone tried to apply for pandemic benefits in her name, which required her to call the government fraud unit to report the fraud, and (v) she had to cancel and replace her debit card due to a fraudulent charge from Apple, which required Plaintiff Hollandsworth to go to the bank half an hour away and sign a sworn affidavit to get a new card as a result." *Id.*, ¶ 113.[2]

Nature of the information. As the Third Circuit pointed out, disclosure of personally identifying information (as opposed to purely anonymous financial information) increases the risk of identity theft. *Clemens*, 48 F.4th at 157. The information here fits this bill—Social Security numbers, private health information, addresses, phone numbers, and email addresses. *Id.* at ¶ 52 ("After an investigation, Highmark determined that the information impacted by the Data Breach included members' Social Security Numbers, and enrollment information such as the

[2] Highmark argues that there are no allegations of misuse because there are no allegations that the hacker here published Plaintiffs' PII/PHI online, or accessed or copied that specific data. ECF 36, p. 12. But that is more of an argument over the nature of the evidence—*i.e.*, direct or circumstantial. The law, of course, makes no distinction between direct versus circumstantial evidence. The Court finds that the amended complaint, at a minimum, pleads reasonable inferences and therefore circumstantial evidence of misuse—for example, by pleading the data breach, the type of information that was accessed, that that type of information is often misused, and then, importantly, instances of misuse of Plaintiffs' information within a close temporal proximity to the data breach (*i.e.*, within a few months).

individual's group name, identification number, and claims or treatment information such as claim numbers, dates of service, procedures, and prescription information, as well as in some cases, financial information, addresses, phone numbers, and email addresses.").

The Court finds that all these factors establish that the injury here, as pled, is plausibly imminent.

Highmark argues that the amended complaint is too speculative on these issues, and that Plaintiffs merely allege that their PII/PHI "may have been exposed or accessed[,]" not that it was actually accessed or actually misused. ECF 36, pp. 10-11.

This argument is a strawman; Highmark reads the Third Circuit's decision in *Clemens* too narrowly. To be sure, in *Clemens*, the company knew who the hacker was, and it was also known when and how the hacker posted the data it stole onto the dark web. *Clemens*, 48 F.4th at 156-57. But that sort of direct evidence isn't required to bestow standing. In fact, it's why the Third Circuit laid out the factors above, and even went so far as to note that evidence of misuse is not required to establish an injury in fact. *Id.* at 154 ("Of note, misuse is not necessarily required.").

True, in this case, unlike *Clemens*, there isn't anything alleged as to who the hacker was or how the hacker used the data. But the amended complaint nonetheless pleads a series of facts and reasonable inferences that the hacker stole the data and even misused it—as noted above, this was a malicious attack, it involved very valuable private information that is often traded on the dark web or used to commit fraud, and within a few months of the attack, one named Plaintiff's personal information appeared on the dark web, and other named Plaintiffs had their credit card accounts hacked. All of this, together, is enough to plausibly allege an injury that is sufficiently imminent.

Turning next to concreteness, the Court finds that Plaintiffs plead a concrete injury. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 426-27 (2021). In the data-breach context, "where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms. For example, if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury." *Clemens*, 48 F.4th at 155-56.

Here, Plaintiffs plead that they spent time and money on mitigation. Several Plaintiffs spent time on scouring credit card accounts, freezing accounts, re-setting passwords, and updating automatic billing. ECF 32, ¶¶ 102-17. One Plaintiff purchased a mitigation service, LifeLock, to mitigate the impact of the fraud. *Id.* at ¶ 113. Plaintiffs also plead that they suffered emotional distress as a result of the breach. *Id.* at ¶ 101.

Highmark contends that this is not enough to establish a concrete injury, as it's all speculative without evidence that the data was actually misused. To begin with, as noted above, a fair reading of the amended complaint suggests that the data was, in fact, misused. But even if it wasn't, the law is now relatively well-settled that loss of time on mitigation efforts, payments made for monitoring, and present emotional distress—all of which are pled here—give concreteness to a plaintiff's injury. *See, e.g.*, *Webb v. Injured Workers Pharm., LLC*, 72 F.4th 365, 376 (1st Cir. 2023) ("The loss of this time is equivalent to a monetary injury, which is indisputably a concrete injury."); *Rauhala v. Greater New York Mut. Ins.,* No. 22-1788, 2022 WL 16553382, at *3 (E.D. Pa. Oct. 31, 2022) (finding standing when the plaintiff alleged

actual identity theft, out-of-pocket expenses associated with the prevention and detection of identity theft, and increased risk of identity theft and fraud).[3]

For these reasons, the amended complaint pleads an imminent and concrete injury in fact.

B. Traceability and redressability.

The second and third requirements for Article III standing (traceability and redressability) have been met here, for largely the same reasons as noted above. Plaintiffs' allegations of misuse outlined above are sufficient to establish a causal link between the data breach and misuse. *Clemens*, 48 F.4th at 158. And the Court can redress any injuries through damages and injunctive relief. *Id.*; *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1141 (C.D. Cal. 2021)

C. Standing for claims for declaratory and injunctive relief.

Standing must be assessed based on each claim alleged and for each form of relief sought. *See TransUnion LLC*, 594 U.S. at 431. That said, the standing analysis above applies in the same manner to all damages claims alleged. *See, e.g.*, *Clemens*, 48 F.4th at 158-59 (applying same standing analysis to contract and tort claims). The claim for injunctive relief, though, requires some additional analysis.

As the Supreme Court "has recognized, a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion LLC*, 594 U.S. at 435. "Where the plaintiff seeks injunctive

[3] Highmark does make a good point that a plaintiff can't just manufacture standing by incurring costs based on fears of a hypothetical harm. *See* ECF 36, pp. 12-13. But that principle goes hand in hand with whether the harm is sufficiently imminent. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013). If the harm is sufficiently imminent—as the Court finds above—then reasonable reactions (*e.g.*, spending time and money on monitoring) to an imminent harm can give rise to a concrete injury.

relief, the allegation of a risk of future harm alone can qualify as concrete as long as it 'is sufficiently imminent and substantial.'" *Clemens*, 48 F.4th at 155. In the data-breach contract, courts have found that plaintiffs have standing for injunctive relief when they allege a real and immediate threat of future injury (*i.e.*, further disclosure of PII). *See*, *e.g.*, *Stallone v. Farmers Grp., Inc.*, No. 21-1659, 2022 WL 10091489, at *9 (D. Nev. Oct. 15, 2022).

Here, Plaintiffs seek injunctive relief "requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect members' PII and PHI." ECF 32, ¶ 219. Plaintiffs allege that without such injunctive relief, they would suffer irreparable injury and lack an adequate legal remedy if another data breach occurs at Highmark. *Id.* at ¶ 220.

Highmark makes two arguments relating to lack of standing. It first argues that any retrospective injunctive relief is improper because Plaintiffs haven't established that they have suffered any present injuries. ECF 36, p. 18. This is just a variation on the same standing argument made with respect to the damages claims, and so the Court rejects it for the same reasons as discussed above.

Highmark's second argument fares better, but is also premature. Highmark argues that Plaintiffs lack standing for any prospective injunctive relief because it is too speculative to say that a second data breach is sufficiently imminent; after all, Highmark discovered this one, and provided notice to the impacted customers. *Id.* at pp. 18-19; ECF 32, ¶¶ 49-54.

The Court finds that some discovery is needed to address this argument, as it will turn on what measures have been put in place by Highmark since the data breach occurred. The amended complaint pleads that the measures remain deficient. ECF 32, ¶ 217. While it's not clear how Plaintiffs actually know this or could know this, at the motion-to-dismiss stage, these sorts of allegations are enough to skate by. *Miller v. Syracuse Univ.*, 662 F. Supp. 3d 338, 357 (N.D.N.Y. 2023) ("Given these

allegations, the Court finds that Plaintiff has sufficiently alleged that he is realistically threatened by another data breach of Defendant's systems, and thus has standing to pursue his requested injunctive relief."); *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d at 1141 ("At the pleading stage, these allegations are sufficient to allege that a data breach is sufficiently likely to recur such that injunctive relief will redress Plaintiffs' injuries.").

That said, the Court's decision here as to the claim for prospective injunctive relief is without prejudice to Highmark to make the same standing argument at summary judgment on a more developed record. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) ("At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim" but "[i]n response to a summary judgment motion, [plaintiffs] can no longer rest on such mere allegations, but must set forth by affidavit or other evidence specific facts, which for purposes of the summary judgment motion will be taken to be true." (cleaned up)).

II. Plaintiffs have sufficiently alleged some claims (Counts I, V, VI, VII) but not others (Counts II, III, IV).[4]

A. Plaintiffs properly state a claim for negligence (Count I).

To plead a claim for negligence under Pennsylvania law, Plaintiffs must allege: "(1) a duty or obligation recognized by the law, requiring the actor to conform to a certain standard of conduct for the protection of others against unreasonable risks; (2) a failure to conform to the standard required; (3) a causal connection between the conduct and the resulting injury; and (4) actual loss or damage resulting in harm to

[4] The parties' briefs make clear that both sides believe that Pennsylvania law applies to these claims. Based on this agreement by the parties, the Court will apply Pennsylvania law and presume that these claims are all claims under Pennsylvania common law.

the interests of another." *N.W. Mut. Life Ins. Co. v. Babayan*, 430 F.3d 121, 139 (3d Cir. 2005).

Highmark argues that Plaintiffs' negligence claim is barred by the economic-loss doctrine and that Plaintiffs fail to plead a cognizable injury because their injuries are speculative or only constitute a risk of future harm. ECF 36, pp. 19-20. Plaintiffs argue that the economic-loss doctrine has an exception where the parties have a special relationship, and that a risk of future harm is a cognizable injury. ECF 38, pp. 18-20. The Court agrees with Plaintiffs.

Turning first to the economic-loss doctrine, "under Pennsylvania's economic loss doctrine, recovery for purely pecuniary damages is permissible under a negligence theory provided that the plaintiff can establish the defendant's breach of a legal duty arising under common law that is independent of any duty assumed pursuant to contract." *Dittman v. UPMC*, 196 A.3d 1036, 1038 (Pa. 2018). The economic-loss doctrine does not preclude negligence claims so long as the defendant owes the plaintiff a common law legal duty to safeguard information that goes beyond a contractual duty. *See, e.g.*, *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 533 (M.D. Pa. 2021) (concluding that "Plaintiffs adequately pled that [defendant] owed them a common law duty to safeguard their credit and debit card information based on [defendant's] affirmative conduct and the foreseeable risk of harm."); *In re Wawa, Inc. Data Sec. Litig.*, No. 19-6019, 2021 WL 1818494, at *5-7 (E.D. Pa. May 6, 2021) (finding that economic-loss doctrine did not bar negligence claim). Under *Dittman*, "those who affirmatively collect sensitive information owe a duty to exercise reasonable care to protect against the foreseeable harm of a data breach." *Opris v. Sincera Reprod. Med.*, No. 21-3072, 2022 WL 1639417, at *4 (E.D. Pa. May 24, 2022). Mitigation damages "are a sufficient form of damages for a negligence claim." *Id.* at *7 (collecting cases).

Here, Plaintiffs have sufficiently alleged that Highmark had a common-law duty to protect their information and that Highmark breached that duty such that the economic-loss doctrine does not apply. Plaintiffs allege that Highmark "had a common law duty to prevent foreseeable harm to others." ECF 32, ¶ 134. Plaintiffs allege that this duty arose from Highmark's position as a healthcare provider tasked with protecting Plaintiffs' information. *Id.* at ¶ 135. Plaintiffs allege that Highmark breached that duty by failing to safeguard their information and that Plaintiffs suffered harm by having their data compromised. *Id.* at ¶¶ 136-38. Highmark affirmatively collected Plaintiffs' PII/PHI in its position as a health insurance and healthcare provider. This gives rise to a common-law duty to prevent foreseeable harm under Pennsylvania law. *See Dittman*, 196 A.3d at 1038; *In re Rutter's Inc.*, 511 F. Supp. 3d at 533. For this reason, the economic-loss doctrine does not bar Plaintiffs' negligence claim.

Highmark's second argument—lack of a cognizable injury—is just a variation of its standing argument. For the same reasons that Plaintiffs' injuries are concrete, they satisfy the injury element for a negligence claim. That is, Plaintiffs allege that they have expended time and money to take steps to try and protect their data after the breach, including spending time looking at credit card accounts, freezing accounts, dealing with actual fraudulent activity, and purchasing protective services such as LifeLock. ECF 32, ¶¶ 103, 106, 109, 113. "These allegations are sufficient to satisfy the damages prong of Plaintiffs' negligence claim at this stage." *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, No. 19-2904, 2021 WL 5937742, at *16 (D.N.J. Dec. 16, 2021). By alleging that they have taken mitigation efforts, Plaintiffs' allegations are sufficient to survive a motion to dismiss. *Opris*, 2022 WL 1639417, at *7.

Accordingly, the Court will deny Highmark's motion to dismiss Count I.

B. Plaintiffs fail to state a claim for negligence *per se* (Count II).

Plaintiffs allege that Highmark violated Section 5 of the FTC Act and HIPAA, and that these violations constitute negligence *per se*. ECF 32, ¶¶143, 145, 150, 152. Pennsylvania does not recognize a claim for negligence *per se* based on statutes without a private right of action, and neither of these statutes provides for private causes of action. *In re Am. Med. Collection Agency, Inc.*, 2021 WL 5937742, at *17 n. 32.

Moreover, negligence *per se* is not a separate cause of action under Pennsylvania law. *Ramsey v. Summers*, No. 10-829, 2011 WL 811024, at *2 (W.D. Pa. Mar. 1, 2011) (Lenihan, M.J.). Instead, it is "a theory of liability that supports a negligence claim." *Simmons v. Simpson House, Inc.*, 224 F. Supp. 3d 406, 417 (E.D. Pa. 2016). This means that a negligence *per se* claim is subsumed in a negligence claim. *Id.* Courts routinely dismiss negligence *per se* claims "as subsumed within the standard negligence claim." *In re Rutter's Inc.*, 511 F. Supp. 3d at 531 (collecting cases). The Court will do the same.

Because the Court has found that Plaintiffs have sufficiently pled their negligence claim, the Court will grant Highmark's motion to dismiss Count II. This is without prejudice to Plaintiffs to advance this theory of liability as part of Count I.

C. Plaintiffs fail to state a breach-of-fiduciary-duty claim (Count III).

"To establish breach of a fiduciary duty in Pennsylvania, the claimant must show: (1) that the defendant negligently or intentionally failed to act in good faith and solely for the benefit of plaintiff in all matters . . . ; (2) that the plaintiff suffered injury; and (3) that the agent's failure to act solely for the plaintiff's benefit was a real factor in bringing about plaintiff's injuries." *Opris*, 2022 WL 1639417, at *10 (cleaned up). Pennsylvania recognizes a fiduciary duty where there is a confidential relationship and the parties "do not deal on equal terms, but, on the one side there is

an overmastering influence, or, on the other, weakness, dependence or trust, justifiably reposed." *Id.* (quotation omitted). "But the mere receipt of confidential information is insufficient by itself to transform an arm's-length transaction into a fiduciary relationship." *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1367 (S.D. Fla. 2015) (collecting cases). The relationship "must go beyond mere reliance on superior skill[.]" *Barletti v. Connexin Software, Inc.*, No. 22-04676, 2023 WL 6065884, at *1 (E.D. Pa. Aug. 17, 2023) (cleaned up). Normally, doctor and patient, principal and agent, trustee and cestui que trust, attorney and client, guardian and ward, and partners are fiduciaries, as a matter of law. *See Harold ex rel. Harold v. McGann*, 406 F. Supp. 2d 562, 571-72 (E.D. Pa. 2005) (collecting cases and listing some examples of fiduciaries under Pennsylvania law). But contracting parties, like an insurer and an insured, are not. *Slapikas v. First Am. Title Ins. Co.*, 298 F.R.D. 285, 293 (W.D. Pa. 2014) (Conti, J.) ("The general rule in Pennsylvania is that insurers do not owe consumers a fiduciary duty.")

Here, Plaintiffs have not alleged the requisite confidential relationship. The amended complaint alleges an insurer-insured relationship.[5] *See, e.g.*, ECF 32, ¶ 2. That's not enough. That said, this doesn't mean that there can never be a fiduciary relationship in an insurer-insured setting; but that would require much more factual development and would probably be quite fact-intensive. *See Yenchi v. Ameriprise Fin., Inc.*, 161 A.3d 811, 824 (Pa. 2017) (reversing the Superior Court's reversal of the

[5] The complaint is a little confusing on this. It names Highmark in its capacity as a healthcare insurer. Yet Highmark (or one of its affiliates) is also obviously a healthcare provider. If the claim here is against Highmark, as a healthcare provider, then the Court's conclusion might be different, as the relationship between Plaintiffs and Highmark might be more akin to a doctor-patient relationship. In several paragraphs, the complaint does refer to Highmark as a "healthcare provider," but that is at odds with how Highmark is otherwise described throughout the complaint. *See* ECF 32, ¶¶ 35, 135, 157, 171 (describing Highmark as "a healthcare provider"); *but see id.* at ¶¶ 2-5, 22, 87, 135, 183(a) (describing Highmark as an insurance provider).

trial court's grant of summary judgment because there was no evidence of a fiduciary relationship). So, the while the Court will dismiss this claim, it will do so without prejudice and with leave to amend, in the event Plaintiffs can plead additional facts to support the existence of a fiduciary relationship.

D. Plaintiffs fail to state a claim for breach of confidence (Count IV).

A claim for breach of confidence "involves the unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship." *Kamal v. J. Crew Group, Inc.*, 918 F.3d 102, 114 (3d Cir. 2019) (cleaned up). The harm underlying a breach-of-confidence action "transpires when a third party gains unauthorized access to a plaintiff's personal information." *Id.*

Importantly, a breach-of-confidence claim requires an affirmative disclosure; failure to safeguard information is not enough. *In re Brinker Data Incident Litig.*, No. 18-686, 2020 WL 691848, at *22 (M.D. Fla. Jan. 27, 2020) ("But [defendant] did not do any act that made Plaintiffs' information known—the information was stolen by third-parties."). A breach-of-confidence claim cannot succeed if the information was stolen and not affirmatively disclosed. *Id.* Finding that a third-party hacker's theft of information constitutes an affirmative disclosure by Highmark is a bridge too far. *Gaddy v. Long & Foster Companies, Inc.*, No. 21-2396, 2022 WL 22894854, at *12 (D.N.J. Mar. 16, 2022) (holding that the proper remedy for the plaintiffs' claim that defendant failed to secure their data was a negligence claim).

Here, Plaintiffs have not alleged that Highmark affirmatively disclosed their information. Instead, the theory of the case is that Highmark "failed to implement reasonable data security measures" to protect their information" and "ultimately allowed nefarious third-party hackers" to access their information. ECF 32, ¶ 27.

That is properly addressed as part of Plaintiffs' negligence claim. *Gaddy*, 2022 WL 22894854, at *12. The Court will grant Highmark's motion to dismiss Count IV.

E. Plaintiffs properly state a claim for breach of implied contract (Count V).

In Count V, Plaintiffs bring a claim for breach of implied contract, alleging that Highmark, through its conduct (specifically its "Notice of Privacy Practices") implicitly agreed to safeguard Plaintiffs' data, and that Highmark breached that agreement when it failed to safeguard the data, leading to the breach here.

Highmark essentially argues that the complaint is too vague; that is, that the complaint doesn't plead the essential terms of the contract (such as Highmark's duties), and pleads no breach. On the breach point, Highmark contends that just because a hacking incident occurred, it doesn't mean that it did anything wrong. The Court agrees with Plaintiffs.

To begin with, "[t]he essential elements of breach of implied contract are the same as an express contract, except the contract is implied through the parties' conduct, rather than expressly written." *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015), *aff'd sub nom. Enslin v. Coca-Cola Co.*, 739 F. App'x 91 (3d Cir. 2018). Corporate policies, such as the Notice of Privacy Practices, can form the basis for implied promises. *See Farmer v. Humana, Inc.*, 582 F. Supp. 3d 1176, 1187-88 (M.D. Fla. 2022) (declining to dismiss a breach of implied contract claim because the plaintiff handed over sensitive information); *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360, 1381-82 (N.D. Ga. 2021) (declining to dismiss an implied contract claim because "Plaintiffs specifically point[ed] to Defendant's Privacy Policy as one indication of Defendant's intent to enter into an implied contract that included a promise to 'reasonably protect' Plaintiffs' private information.").

Here, Plaintiffs plead the existence of the policy, and quote from aspects of the policy that plausibly plead the essential terms of an implied contract—*i.e.*, that

Highmark promised to reasonably protect Plaintiffs' information, including by complying with state and federal privacy laws. ECF 32, ¶¶ 6, 26, 192. Further, Plaintiffs' sufficiently plead breach—*i.e.*, that there was a phishing attack and there were not reasonable measures in place to prevent that. *Id.* at ¶¶ 50, 61, 64. That is enough at this stage, and Highmark's complaints over the claim not having more detail are better suited for after discovery and at summary judgment.[6]

The Court will therefore deny Highmark's motion to dismiss Count V.

F. Plaintiffs properly state a claim for unjust enrichment (Count VI).

Plaintiffs, as an alternative to their implied-contract claim, bring an unjust-enrichment claim. If a complaint includes a breach-of contract claim, a party may include an unjust enrichment claim in the alternative if "the existence or applicability of a contract is in dispute[.]" *Hickey v. Univ. of Pittsburgh*, 81 F.4th 301, 315-16 (3d Cir. 2023). "[I]t is widely accepted practice to pursue unjust enrichment in the alternative at the pleading stage." *Figueroa v. Point Park Univ.*, 553 F. Supp. 3d 259, 275 (W.D. Pa. 2021) (Lenihan, M.J.), *cert. denied*, No. 20-1484, 2021 WL 4975196 (W.D. Pa. Oct. 26, 2021).

To plead a claim for unjust enrichment, Plaintiffs must allege the three elements of unjust enrichment, which are: "(1) conferring a benefit on defendant; (2) defendant's knowledge of the benefit; and (3) circumstances are such that defendant's retention of that benefit would be unjust." *Burrell v. Staff*, 60 F.4th 25, 50 (3d Cir. 2023), *cert. denied sub nom. Lackawanna Recycling Ctr., Inc. v. Burrell*, 143 S. Ct. 2662 (2023).

[6] Plaintiffs linked to Highmark's privacy policy in a footnote in the amended complaint. ECF 32, ¶ 6 n.4. Unfortunately, that link is now unavailable so the Court is unable to examine the language of the policy other than the portions Plaintiffs quote in their complaint.

"[T]he federal courts are not uniform in their analyses of unjust enrichment claims in data breach class actions." *In re Rutter's Inc.*, 511 F. Supp. 3d at 538-39 (reviewing cases and concluding that the Seventh and Eighth Circuits have dismissed similar unjust enrichment claims in the data breach context, but the Eleventh Circuit has upheld them).

The main point of dispute concerns the terms of the bargain. In other words, are Plaintiffs paying for data protection, and does Highmark obtain any benefit associated with the payment that is tied to the data? As one court said in dismissing an unjust-enrichment claim in a case against Jimmy John's, "[the plaintiff] paid for food products. She did not pay for a side order of data security and protection; it was merely incident to her food purchase[.]" *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016). Highmark makes these same arguments, arguing that Plaintiffs here plead that they paid premiums for health insurance; they didn't pay for data security and shouldn't have expected that as part of the bargain. Moreover, Highmark argues that it didn't benefit from the payments in a way that is tied to the data—for example, there are no allegations about how Highmark commercialized the data. The Court disagrees; the complaint is sufficient to state a claim.

As noted above in the context of Plaintiffs' implied-contract claim, the agreement between Plaintiffs and Highmark, as pled, was potentially broader that just a premium in exchange for insurance. As part of the parties' dealings, there was, again, as pled, an agreement to safeguard data and comply with state and federal privacy laws in doing so. And the complaint pleads that part of the premiums paid by Plaintiffs went to Highmark for data security measures—in other words, there was a reasonable expectation that the premiums paid (the benefit) would be for data protection, and thus it would be unjust for Highmark to retain those premiums when it failed to take the right measures to protect the data. ECF 32, ¶¶ 201-206. *Resnick*

v. AvMed, Inc., 693 F.3d 1317, 1328 (11th Cir. 2012) (finding unjust-enrichment claim was appropriately pled where complaint alleged that premiums were partially used for data management and security measures). All of this is enough to state a plausible unjust-enrichment claim at this stage.

Accordingly, the Court will deny Highmark's motion to dismiss Count VI.

G. Plaintiffs properly state a claim for declaratory judgment (Count VII).

The Third Circuit has set forth the following factors for district courts to consider when evaluating declaratory-judgment claims: "(1) the likelihood that the declaration will resolve the uncertainty of obligation which gave rise to the controversy; (2) the convenience of the parties; (3) the public interest in a settlement of the uncertainty of obligation; and (4) the availability and relative convenience of other remedies." *Terra Nova Ins. Co. v. 900 Bar, Inc.*, 887 F.2d 1213, 1224 (3d Cir. 1989) (cleaned up). If there is overlap between a declaratory-judgment claim and other substantive claims, a court can decline to dismiss the declaratory-judgment claim until the record is fully developed. *Opris*, 2022 WL 1639417, at *14.

Here, Plaintiffs seek a judgment declaring that "Defendant owed a legal duty to secure members' PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and Defendant breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI." ECF 32, ¶ 218(a)-(b). The judgment Plaintiffs seek is the same relief that the plaintiffs requested in *Opris*, 2022 WL 1639417, at *14.

In *Opris*, the court declined to dismiss the plaintiffs' declaratory-judgment claim, stating that such a dismissal would be "premature" because "[w]hether the Court should issue such a declaration will depend on the outcome of Plaintiff's substantive claims" which were not fully developed at the motion-to-dismiss stage. *Id.* Courts frequently decline to dismiss declaratory-judgment claims at the motion-

to-dismiss stage when the declaratory-judgment claim overlaps with other substantive claims that have not been fully developed. *Baker v. Deutschland GmbH*, 240 F. Supp. 3d 341, 350 (M.D. Pa. 2016); *Fleisher v. Fiber Composites, LLC*, No. 12-1326, 2012 WL 5381381, at *12-13 (E.D. Pa. Nov. 2, 2012). The Court agrees with this reasoning.

Plaintiffs' declaratory-judgment claim overlaps with several of their other substantive claims, including their breach-of-contract claim and their negligence claim. Because the declaratory-judgment claim overlaps with Plaintiffs' other claims that are not fully developed at this stage of the case, the Court will deny Highmark's motion to dismiss Count VII.

CONCLUSION

Therefore, after careful consideration, it is hereby **ORDERED** that Defendant's motion to dismiss (ECF 35) is **GRANTED IN PART and DENIED IN PART.** A separate order follows.

DATE: April 28, 2025

BY THE COURT:

/s/ *J. Nicholas Ranjan*
United States District Judge